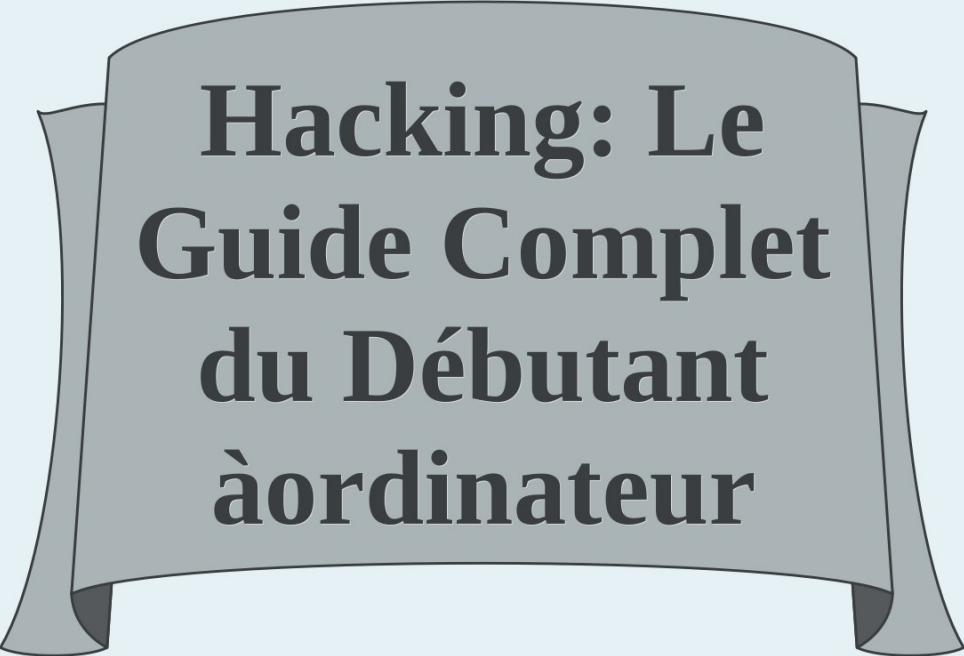




Hacking: Le Guide Complet du Débutant à ordinateur

Miles Price

VISIT...

LANZAROTE
Caliente.COM



HACKING

LE GUIDE COMPLET DU
DÉBUTANT À ORDINATEUR
PIRATAGE ET TESTS PÉNÉTRATION

MILES PRICE

Hacking

*Le Guide Complet du Débutant à ordinateur Piratage
et Tests Pénétration*

Miles Price

Tableaude matières

Introduction

Chapitre 1: Il estmonde d'Hacker!

Chapitre 2:Test

Chapitre 3pénétration:Méthodologie de The

Chapitre 4Hacker:Obteniraccès physique

Chapitre 5:ingénierie sociale

Chapitre 6: Piratagemotspasse

Chapitre 7: Réseau sans fil Attacks

Chapitre 8: Piratageun Smartphone

Chapitre 9: Piratage Conseils pourdu débutant

Conclusion

ressources

Présentation

Cybercriminalité est la plus grande menace que chaque organisation sur la planète fait face aujourd'hui! Et ce n'est pas seulement les organisations qui sont vulnérables, gens sont trop à risque d'être ciblés par pirates.

Dans ce livre nous voulons vous montrer l'importance de rester au-dessus de cette menace en apprenant comment pirater. Il est vrai que pirates ont reçu une mauvaise réputation ces dernières années, principalement à cause de reportages des médias biaisés, tous pirates ont des intentions criminelles.

Ce livre est destiné à servir de guide pédagogique pour gens qui sont intéressés à apprendre des outils de piratage simples, astuces et techniques afin de vous protéger et protéger vos réseaux informatiques.

Il doit être utilisé pour piratage éthique et non activités malveillantes. Si vous avez déjà été curieux de piratage et ont voulu apprendre l'art du hack, alors vous avez trouvé le bon livre.

Nous vivons dans un monde où tout est interconnecté. Retour dans la journée, nous nous sommes appuyés sur les organisations gouvernementales et grands pour fournir suffisamment de sécurité pour nos données personnelles. Ce n'est plus possible dans un monde où les agences de sécurité elles-mêmes sont les principales cibles des pirates.

En fait, dans la plupart des cas, la plus grande menace cybernétique viendra de votre propre gouvernement!

Donc que fais-tu? Asseyez-vous et croisez les doigts, espérant que votre pare-feu et antivirus sera suffisant pour vous protéger? Que vous vouliez ou non, vous devrez apprendre à pirater si vous allez avoir une chance de garder vos propres systèmes de cybersécurité.

En comprenant comment pirates malveillants font ce qu'ils font, vous serez en mesure de détecter et prévenir les menaces potentielles à un système informatique ou réseau. Ce livre vous aidera à faire.

Nous commençons par un aperçu général de l'état de sécurité mondiale cybernétique. Vous apprendrez à faire une distinction entre les différents types de pirates là-bas, leurs motivations et les compétences que vous avez besoin pour commencer le piratage tout seul.

Nous couvrirons également comment effectuer des tests de pénétration pour vérifier toutes les lacunes potentielles dans un réseau. Chaque

réseau, quelle soit la sécurité, a une sorte de faiblesse. Vous apprendrez ce qui se passe dans le ciblage, la numérisation et l'analyse d'une cible, et comment accéder à un système.

Il existe différentes façons de pirater un système informatique. Nous prenons un regard en profondeur sur certaines des tactiques haut niveau qui utilisent des pirates malveillants pour lancer des attaques sur leurs cibles. Enfin, que pouvez-vous faire pour rester sécurisé comme un hacker? Lisez tout cela et plus ici.

Ce livre a été traduit par un logiciel automatisé pour atteindre un public plus large. S'il vous plaît ignorer une traduction erronée.

Je vous souhaite le livre!

© Copyright 2017 - Tous droits réservés.

Le contenu de ce livre ne peut être reproduite, dupliques ou transmis sans autorisation écrite directe de l'auteur.

En aucun cas, aucune responsabilité légale oublâme lieu contre l'éditeur pour une réparation,dommages oupertes financièresraison des informations présentes,soit directement ou indirectement.

Mentions légales:

Ce livre est protégécopyright. Ceci est seulement pourusage personnel. Vous ne pouvez pas modifier, distribuer, vendre, utiliser, devis ou paraphraser tout ou partie du contenu de ce livre sans le consentement de l'auteur.

Avertissement Avis:

S'il vous plaît noter les informations contenues dans ce document sont àfins éducatives etdivertissement seulement. Tousefforts ont été faits pour fournirexactes, à jour et complètes fiables. Aucune garantie de quelque nature qu'elle soit explicite ou implicite.lecteurs reconnaissent que l'auteur ne se livre pas dans le rendu des conseils juridiques, financiers, médicaux ou professionnels. Le contenu de ce livre a été dérivé de sources diverses. S'il vous plaît consulter un professionnel agréé avantessayer des techniques décrites dans ce livre.

En lisant ce document, le lecteur accepte queen aucun cas, l'auteur est responsable des pertes, directes ou indirectes, qui sont engagés à la suite de l'utilisation deinformation contenue dansprésent document, y compris, mais sans s'y limiter, -errors , omissions ou inexactitudes.

Chapitre 1: Il est monde d'Hacker!

Les jours de repos sachant facile que vos informations privées établi des regards indiscrets sont plus! Le monde nous vivons actuellement n'est plus ce qu'il. La cybercriminalité est une menace réelle, dangereuse et persistante que chaque organisation et besoins individuels à prendre sérieux. Ce moment nous vivons à l'ère numérique et dans un village global. Avec tout et tout monde interconnecté à une telle échelle masse, il est sûr de dire que c'est le monde d'un pirate informatique.

Le nouveau président américain lui-même, Donald Trump, a déclaré que vol de cyber est le crime plus rapide plus en Amérique. Ce n'est pas son opinion personnelle. La communauté de sécurité informatique accorde aussi.

Vous ne me croyez pas? Voyons quelques statistiques.

1. Saviez-vous que les dommages causés par cybercriminalité en 2016 coûté 3 billions \$, et devrait atteindre 6 billions \$ l'année à l'an 2021?
2. Saviez-vous que organisations partout aux États-Unis dépensé un total de 80 milliards \$ sur produits et services pour se protéger contre la cybercriminalité? Ce chiffre devrait dépasser 1 billion \$ en 2017.
3. Saviez-vous qu'il n'y a pratiquement aucune chance de chômage si vous travaillez dans l'industrie de sécurité informatique ce moment? Les analystes ont conclu qu'il ya une pénurie extrême de talents de cybersécurité partout dans le monde, le taux de chômage de sécurité informatique tomber à zéro à partir de 2016!
4. Les pirates sont maintenant pressés, passifs. Selon Microsoft, il y aura 4 milliards de personnes en ligne à l'an 2020, humains, ordinateurs, sont maintenant la principale cible des pirates.
5. Saviez-vous que le pirate moyen mesure de rester assis dans votre réseau pour une moyenne de 200 jours sans être détecté?

Ces statistiques ne sont pas destinées à vous faire peur. Ils sont destinés à ouvrir les yeux sur ce qui se passe partout dans le monde. Si vous regardez et lisez les nouvelles, vous devez comprendre l'ampleur du problème prendra l'avenir.

Hacking Défini

Ce qui vient à votre esprit quand vous entendez le mot « piratage? » Imaginez-vous un personnage capuchon penché sur un ordinateur essayant d'obtenir accès illégal à un réseau pour voler des données? Ou peut-être un peu intello geeky avec rien à faire toute journée mais envoyer des programmes cryptés pour infecter réseaux et systèmes?

Quelles que soient les images peuvent avoir sauté dans votre tête, le fait est que la plupart des gens croient que tous les pirates ont l'intention de voler des informations ou d'espionner des gens. La majorité des gens pensent que tous les pirates sont criminels et que le piratage est mauvais. Cela peut être ce qui est dépeint dans les films et émissions de télévision, mais il est tout simplement pas le cas.

Hacking peut être définie comme une tentative de résoudre un problème ou améliorer une application par matériel ou logiciel réingénierie. En d'autres termes, si vous avez un problème avec votre ordinateur et ne parvenez pas à résoudre le problème utilisant des techniques classiques, alors vous pouvez être forcé d'utiliser une technologie est disponible mais d'une manière nouvelle. Si vous regardez l'histoire de la façon dont le piratage a commencé, tout a commencé avec l'intention de résoudre un problème utilisant des moyens créatifs.

Les premiers enregistrés « pirates » étaient un groupe de geeks MIT qui ont utilisé l'ancien équipement téléphonique pour contrôler leur modèle de trains retour dans les années 1950. Ces gars là étaient tellement en forme qu'ils ont pris l'équipement téléphonique qu'ils avaient reçu comme un don et conçus pour que plusieurs opérateurs puissent contrôler la voie ferrée en composant simplement le téléphone.

Certains de ces gars là même allés plus loin et ont commencé à modifier les programmes informatiques récemment mis en place sur campus. Leur objectif était de personnaliser les programmes pour usage spécial et rendre mieux. Ils ont simplement utilisé ce qu'ils avaient à disposition de faire preuve de créativité, inventer une nouvelle façon de faire quelque chose, et résoudre des problèmes.

C'est ce que hacking est sur. Aujourd'hui, le piratage peut représenter une violation de la cybersécurité, des systèmes dommageables et un accès illégal, mais ce n'est pas toute l'histoire.

Alors comment distinguez-vous les bons gars des criminels?

La psychologie de Hacking

Pour arrêter un hacker, vous devez d'abord comprendre ce qui les motive. Dans la communauté du piratage, il y a plusieurs niveaux de compétences diverses et complexes et motivations. Il est important que vous compreniez les différents types de pirates informatiques afin que vous puissiez évaluer de prédire leurs tentatives et comprendre leur mentalité. Même tant que débutant qui apprend comment pirater un système, vous ne voulez pas vous laisser vulnérable à une contre-attaque.

Catégories de pirates

Les plus gros erreurs que font les pirates dans le même groupe que si elles ont un seul but. Cela est souvent ce que les médias font, et le public est tombé pour ce mensonge. Vous ne pouvez pas tenter de classer un pirate sans savoir pourquoi ils ont joué le hack et quels leurs objectifs étaient. La communauté du piratage est quelque peu divisée sur la façon de nommer différents types de pirates, mais en général, ce sont les catégories que la plupart d'accord sur :

- **White Hats** - également connu comme *«hackers éthiques»*, ces pirates opèrent dans la loi. Ils collent à l'éthique du hacker, qui stipule qu'un pirate doit « ne pas nuire ». Ils travaillent aussi comme experts de sécurité cybernétique et sont embauchés pour détecter des vulnérabilités potentielles dans un système ou réseau, et les corriger. Ce type de pirate informatique travaille avec des éditeurs de logiciels pour patcher une vulnérabilité dans leur logiciel. Les chapeaux blancs font généralement ce qu'ils font tant que service public. Leur but est de sensibiliser le public aux menaces là-bas afin que les gens sachent comment un système est vulnérable. Cependant, ils ne publient publiquement ces données jusqu'à ce que le fournisseur du logiciel a fait eux-mêmes.

- **Black Hats** - Ce type de pirate est souvent convaincu qu'ils sont en train de faire un service public, mais en réalité, leur principale motivation est le pouvoir et l'argent. Ils ont tendance à pénétrer les réseaux afin qu'ils puissent voler ou endommager les données. Ils sont animés par une haine ou colère malveillante contre une organisation ou pays. Il est intéressant de noter qu'ils ont obtenu leur nom du fait que des méchants dans la plupart des films occidentaux cowboy portaient des chapeaux noirs.

- **Gris Chapeaux** - Ce terme a été initialement présenté par un groupe de pirates d'une vieille école très célèbre qui ne voulait pas être associé avec les chapeaux noirs ne sont pas encore désireux de être stigmatisés comme testeurs de sécurité d'entreprise. Les chapeaux gris

peuvent être décrits comme pirates qui ont utilisé comme Black Hats mais ont reformé et travaillent maintenant comme experts en sécurité informatique. Ils sont parfois définis comme pirates qui consultent ainsi que accès illégal aux gains réseaux.

Classes de pirates

Il y a des classes spécifiques qui relèvent des catégories de pirate Chapeau noir et blanc mentionnés ci-dessus. Ceux-ci comprennent :

- **Elite** - Ce sont les gourous du monde du piratage. Ils ont les compétences et connaissances personnelles n'ayant d'autre. Mais ce qui les rend extrêmement rare est leur éthique et l'intégrité. Ils agissent souvent comme White Hats qui connaissent l'infrastructure réseau et possèdent les connaissances de programmation pour écrire leurs propres outils. Ils ne sont pas motivés par des intentions criminelles et sont plus intentionnellement détectés pour des problèmes de codage ou de failles de sécurité et informer les administrateurs système. Vous ne pouvez devenir un hacker elite en effectuant un hack bien connu ou exploiter ou maintenir longtemps tant que pirate.

- **Cyberterroristes** - Cette classe de pirate va au-delà d'écraser un réseau utilisant un déni de service (DoS). Ils se développent et aiment le fait qu'ils peuvent cacher derrière le voile du Web comme ils partagent l'information entre eux. Ils sont capables de cacher des données chiffrées dans une sorte que seul un homme cyber criminel peut trouver. Les gouvernements partout dans le monde ont tendance à embaucher ces types de pirates pour faire leur sale affaire, allant de l'espionnage simple à la cyberguerre.

- **Script Kiddies** - Personne est aussi décrié ou ridiculisé comme script kiddie. Cette classe de pirate est jeune, inexpérimenté, et non qualifiée pour créer leurs propres outils à exploiter. Ils utilisent des outils fabriqués par des pirates élites, et ne peuvent pirater des systèmes que d'autres ont relevé des vulnérabilités. Ils piratent la plupart du temps pour le plaisir et sont ceux dont les exploits sont souvent mentionnés dans les médias. Leurs principales réalisations sont généralement des attaques DoS et des pages web défigurées.

- **Hacktivistes** - Ceci est une combinaison d'un hacker et d'un activiste. Ils portent des programmes politiques, sociaux ou religieux et peut être très tenace. Ils définissent des sites Web et effectuent des attaques DoS à faire pression sur les gouvernements ou les organisations qu'ils considèrent causer des dommages à un groupe particulier de la société.

● **Employé scolaire** - Ce sont gens qui ont connaissances intérieures d'une organisation et utilisent leur accès à recueillir information pour eux-mêmes ou autres. Ils sont considérés comme extrêmement dangereux même si le public est rarement en entendre parler. Ces pirates sont généralement calmes et timides mais ont des personnalités narcissiques. Ils tournent sur leurs employeurs chaque fois qu'ils croient qu'ils ne sont pas reconnus pour leur travail.

● **auteurs de virus** - Ce sont gens qui profitent de toutes faiblesses qu'un pirate informatique a exposés, et vont à écrire code pour exploiter ces vulnérabilités.

Compétences requises pour Hacking

tant que débutant, il y a des compétences base que vous devez développer si vous êtes à progresser dans le monde du piratage informatique. Ceuxci comprennent:

1. **Outils informatiques maîtrisés** - Vous devez être informés dans utilisation des ordinateurs et être mesure de comprendre instructions écrites. Naviguer sur Internet sans but ne compte pas. Pouvezvous utiliser le module de commande Windows? Ces compétences base sont essentielles pour chaque pirate valeur leur sel.
2. **bonne connaissance de Linux OS** - Linux vous permet de personnaliser vos programmes, qui explique pourquoi pirates préfèrent sur Mac et Windows.
3. **Compétences de base de données** - Apprendre à utiliser systèmes de gestion de bases de données comme Oracle et MySQL vous aider comprendre comment pénétrer bases données.
4. **Compétences réseau** - tant que pirate informatique qui sera engagé dans beaucoup d'activité ligne, vous devez savoir sur concepts tels sous réseaux, DNS, ports, mots passe WPS, et ainsi suite.
5. **Compétences de script** - Vous ne pouvez pas savoir comment le code ce moment, mais tôt ou tard vous devrez apprendre. Chaque pirate besoin d'avoir leurs propres outils de piratage plutôt que dépendre de ce que autres ont créé. se fondant sur outils faites par autres pirates laisse votre système vulnérable à exploitation. Prenez temps d'apprendre quelques langages de script tels que Ruby on Rails ou Python.
6. **Compétences en ingénierie inverse** - un des moyens les plus efficaces pour développer un outil de piratage informatique est de prendre un existant, démonter, et trouver un moyen de faire mieux. Ces compétences sont inestimables pour un pirate informatique.
7. **utilisation de logiciels de virtualisation** - Ce type de logiciel permet de tester toute sécurité votre hack sur votre ordinateur avant lâcher sur quelqu'un autre. Un bon exemple est VMWare Workstation.

Qu'est-ce qu'une motivation d'un Hacker?

Il faut que les opérations de piratage ont été menées par un collègue ou cachette pour adolescents du secondaire au soutien de leurs parents. Nos jours, les cyberattaques sont plus sophistiquées et à grande échelle. Pourtant, malgré le fait que la cybercriminalité a progressé à un rythme alarmant avec une meilleure technologie, les motivations du hacker d'aujourd'hui ne diffèrent guère de celle de la génération précédente.

Donc ce qui motive un cybercriminel à pirater un réseau ou système? Il y a quatre raisons fondamentales:

1. **argent** - le gain financier est le plus grand facteur de motivation. La plupart des cyberattaques d'aujourd'hui. Vous avez entendu parler de pirates exploitant les vulnérabilités du système des institutions financières et de partir avec des numéros de cartes de crédit, comptes de messagerie, mots de passe, noms d'utilisateur, etc. Un hacker malveillant va vendre tout ce qu'ils peuvent trouver pour un prix. Certains chapeaux noirs même des organisations de chantage à l'aide de ransomware.
2. **Agenda politique / Idéologique** - C'est là que les hacktivistes tombent sous. Ils attaquent les réseaux d'institutions gouvernementales, les organisations et les personnalités de premier plan pour faire avancer leurs programmes idéologiques, politiques, sociaux ou scientifiques. Un groupe connu pour avoir de telles motivations sont les anonymes.
3. **Divertissement** - La majorité des chapeaux gris ont tendance à exploiter les réseaux pour le plaisir ou l'orgueil. Ils cherchent un défi et la violation des lois éthiques pour satisfaire leur curiosité. Cependant, ils ne sont pas malveillants et vont même informer l'administrateur du réseau sur les vulnérabilités qu'ils trouvent.
4. **Cybersécurité** - Les White Hats utilisent généralement un système d'exploitation pour trouver des faiblesses afin qu'ils puissent les rendre plus sûres. Les organisations emploient souvent des pirates de travailler pour eux, les vulnérabilités de patch, et créer des codes de pratique pour les employés à suivre pour éviter d'être atteints par le cyber.

Chapitre 2: intrusion tests

Testspénétration fait référence à l'essai d'un système cybernétique, réseau ou application pour détecterfaiblesses qui peuvent être exploitées par un pirate malveillant. Vous essentiellement essayez d'accéder à un système sans avoir de nomsutilisateur ou motspasse. L'objectif est de voir comment il est facile d'obtenirinformations confidentielles sur une organisation, puis augmenter la sécurité du système testé.

Alorsquelle est exactement la différence entre un test de pénétration et une attaque? permission!

Un pirate informatique qui effectue un test de pénétration sera donné l'autorisation par le propriétaire du système, qui sera ensuite attendre un rapport détaillé à la fin de tout.tanttesteur, on peut vous donner accès au niveau utilisateur pour vous permettre d'entrer dans le système.partirlà, vous devrez vous attendre à voir s'il est possible d'avoir accès àinformations confidentielles qu'un utilisateur ordinaire ne devrait jamais voir.

L'autre option est d'aller en aveugle. Dans une évaluation aveugle ou secrète, vous n'êtes pas donné des informationsexception du nom de l'organisation cliente. Le reste est à vous,qui est exactement commentpiratesplus malveillantsfonttoute façon. Le seul problème avec une évaluation secrète est que cela prendra plustemps qu'un un manifeste,augmente les chances de vous manquer une faille.

Vous pouvez être embauché pour trouver une seule faiblesse, mais dansplupartcas, vous serez appelé à continuerchercher pour trouver toutes les vulnérabilités potentielles dans un réseau. Une fois identifié, vous devrez trouvermoyens de fixationces trous. Ceci estraisonlaquelle vous devrez écrireunotes détaillées concernant votre procédure de test etrésultats.prisenotes permet au client de déterminer l'efficacité de votre travail et vérifier si les problèmesvous avez découverts sont bien fixés. Cependant, il est très peu probable que vous détecter tousdéfauts de sécurité unique outrou dans le système.

détectionvulnérabilités

Les mesures prises par un testeur de pénétration et un hacker malveillant sont généralement les mêmes. Dansplupartcas, un hacker malveillant se déplace lentementtravers un système afin d'éviterêtre détectés. Vous pouvez également suivre la même tactique pour voir à quel point efficace le système d'un client est à détectertelles attaques. Une fois cela fait, ces lacunes doivent être scellés.

La première étape est généralement reconnaissance. Vous essayez de recueillir autantinformations sur votre réseau cible que vous le pouvez. Ceci est normalement un processus passif qui consisteutiliserressources disponibles au public. Vous pouvez identifier les serveurs Web de l'organisation, OSil estcoursexécution, la version du logiciel, patchs ou modules serveur a permis,adresses IP, et dans certains cas, même le nom du serveur interne.

Lorsque vous avez rassemblé vos informations, il est alors temps devérifier. Ceci peut être réalisé en comparant les informations de réseau ousystème avecvulnérabilités connues recueillies. Une foisvous tester les vulnérabilités, vous saurez avec certitude si les informationsvous aviez recueillies sont exactes ou non.

Raisons pour effectuer des tests de pénétration

1. Identifier les faiblesses que les pirates mal intentionnés pourraient

Même que vous lisez ce livre ce moment, il est possible qu'il y ait des pirates malveillants lancent des outils et attaques de réseau pour tenter de pénétrer votre système. Ces attaques sont sans fin et vous ne pouvez pas prédire quand un système sera touché. Dans la plupart des cas, ces exploits sont bien connus et donc évitables. Le service informatique d'une organisation peut être désireux de savoir où sont les faiblesses de son réseau et comment un hacker malveillant peut tirer profit. En tant que testeur de pénétration, vous devrez attaquer le système et fixer les trous avant que quelqu'un avec de mauvaises intentions trouve leur chemin. Un système peut être sécurisé aujourd'hui mais demain il peut être victime d'une violation.

1. Justifier la gestion du besoin de ressources

Il y a des moments où la haute direction ne voit pas seulement la nécessité d'allouer davantage de ressources financières vers la sécurité cybernétique. Dans ce cas, les tests de pénétration est la meilleure façon pour l'équipe de sécurité de l'entreprise pour justifier leurs demandes de plus de fonds. L'équipe de sécurité informatique peut être en courtisant des vulnérabilités mais la gestion résiste à l'appui des changements apportés au système existant. En externalisant les tests à un consultant externe, la gestion est plus susceptible de respecter les résultats obtenus.

1. Assurez-vous que l'équipe de sécurité interne fait son travail

Le rapport de test de pénétration montrera si le ministère de sécurité informatique est efficace dans son travail. Il peut déterminer s'il y a un écart entre les connaissances des vulnérabilités du système et la mise en œuvre des mesures de sécurité.

1. formation du personnel du réseau

Imaginez si un pirate devait avoir accès au système d'une organisation sans le personnel même savoir. En effectuant un test de pénétration, il est possible de découvrir à quel point vigilant votre sécurité et si le personnel a besoin d'information supplémentaire. Il met également en évidence l'efficacité des contre-mesures qui ont été mises en place en cas d'une cyberattaque.

1. Test des nouvelles technologies

Avant lancer un nouveau morceau de technologie, par exemple, une nouvelle infrastructure sans fil, il est essentiel que le système est testé pour vulnérabilités. Cela va certainement économiser plus d'argent que d'effectuer le test tandis que les clients utilisent déjà.

Le Rapport test pénétration

Une fois vous avez terminé le test, vous devez compiler toutes les données dans un format approprié et soumettre un rapport. Gardez à l'esprit que la majorité du personnel de gestion ne peut pas être orienté technique, sorte que le rapport doit être divisé en sections appropriées pour faciliter la lecture. Vous devriez avoir un résumé, un résumé technique contenant tout le jargon spécifique, et un résumé de gestion qui explique ce qui doit être fait pour corriger les défauts détectés.

Chapitre 3: La méthodologie du Hacker

Imaginez un soldat dans un champ de bataille entièrement équipé dans les armes les plus récentes et les plus avancées. Ils sont pleins de confiance et savent avec certitude qu'ils vont gagner. Cependant, lorsque le combat commence, le soldat découvre qu'il est entré dans une embuscade. Il peut descendre la plupart des troupes ennemies, mais parce qu'il n'a jamais été préparé pour la bataille, il finit par perdre.

Ce scénario est pas si farfelu si on considère le nombre de soi-disant « pirates » qui ne prennent pas le temps de préparer à leurs attaques. C'est là que la méthodologie de piratage est très pratique.

Une méthodologie de piratage est ce qu'un pirate utilise pour les guider de la première étape à la dernière. Pour exploiter efficacement une vulnérabilité dans un système, vous devez identifier quelques éléments clés qui vous aideront à atteindre vos objectifs. Sans une méthodologie appropriée, vous risquez de finir par perdre du temps et la lutte contre une énergie perdue d'avance.

Cartographie cible

Trouver la cible parfaite pour votre attaque est pas aussi simple que cela puisse paraître. Vous devez être stratégique dans la façon dont vous menez votre recherche et effectuez recherche sur la cible avec le plus potentiel. Vous devez analyser leurs habitudes et utiliser les informations recueillies pour trouver la stratégie plus appropriée. L'objectif de cartographier votre objectif est de déterminer quoi et qui vous attaquez avant pénétrer le système.

Pirates informatiques vont généralement après une ou plusieurs cibles à la fois. Selon le type d'information que vous recherchez, vous pouvez décider d'attaquer serveurs Web stockant informations personnelles. Vous pouvez également décider d'aller grand et pirater une institution financière. Votre cible pourrait être un site Web spécifique que vous voulez prendre à l'aide d'attaques déni, ou vous pouvez défigurer sa page Web. Vous pouvez être intéressé par une personne particulier dans une organisation.

Lorsque vous êtes recherche de cibles potentielles à l'attaque, vous devez considérer le niveau de sécurité que vous allez essayer de surmonter. La plupart des pirates vont seulement après des cibles qu'ils connaissent sont faciles à battre, sorte que le niveau de vulnérabilité est souvent un facteur clé dans la cartographie de votre cible.

Un autre facteur à considérer est savoir si les informations obtenues de l'attaque est précieuse. Cela vous aidera à déterminer combien de temps vous êtes prêt à passer à essayer d'accéder au système.

Alors comment allez-vous recueillir des informations sur votre cible?

● Effectuer des recherches en ligne

Vous pouvez Google le nom de la cible et vérifier leur compte Facebook ou LinkedIn. Cela peut faire apparaître leurs coordonnées. Si votre cible est une organisation, vous pouvez rechercher des offres d'emploi que l'entreprise a annoncées pour particulier dans le département informatique. Vous pourriez être surpris d'apprendre à quel point des informations utiles est donnée dans une offre d'emploi, par exemple, le logiciel que recrues potentielles doivent connaître.

Tant que hacker, vous devez savoir quels mots clés apporteront le plus d'informations. Utilisez de Google de recherche avancée fonction afin d'identifier les sites qui ont des backlinks dans le site de votre cible. Si vous souhaitez accéder à tous les fichiers qui peuvent être dans le site Web d'une entreprise, vous devrez utiliser un commutateur comme indiqué ci-dessous:

site: www.abc.com mot-clé

Autre technique à utiliser est l'outil WHOIS. Whois est un excellent moyen d'effectuer une attaque d'ingénierie sociale ou scannez un réseau. Vous pouvez trouver les serveurs DNS du domaine cible, ainsi que les noms et adresses des personnes qui ont enregistré le domaine cible.

Google Groupes tendance à stocker beaucoup de données sensibles sur ses utilisateurs, par exemple, noms d'utilisateur, noms de domaine et adresses IP.

● Ramper Web

Acquire ce qu'on appelle les « outils d'exploration Web » pour créer une image miroir du site cible. Une fois vous avez fait cela, tous les fichiers du site qui est accessible public sera téléchargé sur votre disque dur local. Cela vous permettra de numériser la copie miroir et trouver les noms et adresses email des employés, fichiers, répertoires, le code source pour ses pages web, et beaucoup plus d'informations.

● Sites

Vous devriez maintenant être conscient qu'il ya certains sites qui sont un trésor d'informations clés sur individus et organisations. bons exemples comprennent www.sec.gov/edgar.shtml, www.zabasearch.com et www.finance.yahoo.com.

Numérisation réseau cible

Jusqu'à présent vous avez été collecteur d'informations qui vous permettra de voir l'ensemble du réseau cible dans son ensemble. Les noms d'hôtes, ports ouverts, adresses IP et applications en cours devraient maintenant être visibles pour vous. Rappelez-vous que si vous êtes d'effectuer un efficace exploit, vous devez apprendre à penser comme un hacker malveillant.

Vous pouvez commencer à utiliser un logiciel de numérisation pour trouver et enregistrer tous les hôtes qui sont accessibles en ligne. Votre propre système d'exploitation devrait avoir son propre outil de ping standard. Cependant, il existe des outils tiers comme SuperScan et outils NetScan Pro qui sont capables de ping le nom d'hôte du domaine ou plusieurs adresses IP simultanément.

Analyseports ouverts

Tant que débutant, il existeoutils que vous pouvez utiliser pour vérifier la présence de ports ouverts pour pénétrerle réseau cible.exemples de certains outils efficaces comprennent SuperScan, Wireshark, et OmniPeek.

Expositionvulnérabilités système

Supposant quevous trouvezcertaine vulnérabilité dans le système de votre cible, vous pouvez alors commencervérifier si ces lacunesmatière de sécurité sont exploitables. Vous pouvez suivre la voie manuelle ou utiliser un outil d'évaluation automatique.

La méthode manuelle vous demandera de créerlien versun des ports ouvertsvousdécouvert plus tôt. . Testez ces ports jusqu'à ce que vous trouviez un moyen de

la méthode automatisée implique l'utilisation d'outils tels que *QualysGuard*,qui est un outil basé sur le nuage qui est conçu pour scannerports ouverts. Un autre outil qui est disponible est Nexpose, qui peut numériser un total de 32 hôtes simultanément.

Chapitre 4: Obtenir accès physique

Imaginez: Une société de plusieurs millions de dollars investit millions de dollars sur des mesures de sécurité cybernétique axée sur la technologie pour protéger ses données. Ils ont totalement verrouillé leurs réseaux et systèmes, et ont mené plusieurs tests de pénétration utilisant des pirates d'élite pour protéger des pirates qui peuvent avoir été engagés par leurs concurrents.

Maintenant imaginez que cette société continue d'embaucher une entreprise de sécurité qui engage des gardes de sécurité paresseux. Ils ne font jamais de contrôles physiques autour de l'installation et même laisser des portes ouvertes. Les visiteurs sont rarement analysés ou invités à se connecter. Même les salles informatiques sont généralement laissées ouvertes.

Diriez-vous que c'est une entreprise intelligente qui prend soin de protéger ses données contre les pirates? Oui, ils ont branché les trous électroniques, mais ils ont littéralement laissé la porte ouverte pour les pirates d'ouvrir une brèche physiquement leur sécurité!

Vous n'avez pas à pirater un réseau à distance pour accéder aux données. Vous pouvez avoir accès physique à une installation et effectuer votre exploit de l'intérieur. Cours des deux dernières décennies, la plupart des entreprises ont constaté qu'il est extrêmement difficile de maintenir la sécurité physique. Merci aux progrès de la technologie, il y a maintenant des vulnérabilités plus physiques qu'un pirate peut tirer profit.

Dans le monde d'aujourd'hui des lecteurs USB, tablettes, smartphones et ordinateurs portables, plus en plus de données sont stockées dans des appareils plus petits et portables. Il est pas difficile de mettre la main sur tels dispositifs, en particulier compte tenu du fait que la plupart des employés prennent des données avec eux quand ils quittent le travail à la fin de la journée. Une fois que vous identifiez votre cible, vous ne pouvez pas même avoir à entrer le bâtiment; ils apporteront les données pour vous.

Dans ce chapitre, vous allez apprendre davantage sur la façon de tirer parti de certaines des failles de sécurité physique dans les bâtiments que vous avez ciblés. Une fois que vous avez violé la sécurité et obtenu l'accès physique acquis sur place, préparez-vous à pénétrer le système de l'intérieur.

Types de vulnérabilités physiques

- non d'établir une réception pour surveillervisiteurs qui entrent et sortent du bâtiment.
- non-application signature dans obligatoire de tous employés et visiteurs.
- employés et personnel de Distant sécurité qui ne sont pas complètement familiers avec les réparateurs informatiques, fournisseurs ou fournisseurs.
- Jetant documents entreprise et personnels sensibles à la poubelle lieu de les déchiqueter.
- non-verrouillage portes menant à salles informatiques.
- Laisant appareils numériques trouvant dans les bureaux.
- défaut de fixer portes qui ne peuvent pas fermer correctement.

Créer votre plan

une des premières choses vous aurez à faire est de trouver un moyen d'atteindre la sécurité physique. Cela nécessitera un travail vaste de reconnaissance de votre part. Vous devez identifier le type de mesures de sécurité que l'installation a mis en place, les faiblesses et vulnérabilités présentes, et comment tirer profit.

Cela peut sembler simple sur papier mais il n'est pas si facile une fois vous obtenez sur le terrain. L'hypothèse ici est que vous travaillez sans homme intérieur de vous nourrir les informations vitales de sécurité. Il peut être deux ou trois semaines avant vous êtes mesure de recueillir toutes les informations vous avez besoin pour lancer votre attaque. Une atteinte à la sécurité physique signifie vous devez avoir les compétences et connaissances nécessaires pour non seulement entrer le bâtiment, mais aussi pour manœuvrer votre chemin intérieur, puis sortir sans être détecté.

Si vous manquez la patience, condition physique et agilité mentale nécessaire pour une telle tâche, alors ne pas tenter une violation physique. Tenez-vous d'effectuer vos attaques à distance.

Il y a un certain nombre de facteurs de sécurité physique que vous devrez tenir compte lors de la planification comment accéder à votre cible. Ceux-ci sont classés en deux catégories distinctes : contrôles physiques et contrôles techniques.

Contrôles physiques

Vous aurez à prendre compte la façon dont les contrôles de l'équipe de sécurité, surveillance et gestion des accès dans et hors de l'établissement. Dans certains cas, le bâtiment peut être divisé en sections publiques, privées et restreintes. Vous devrez déterminer la meilleure technique pour entrer la section qui contient la cible.

1. Périmètre de sécurité

Comment prévoyez-vous contourner la sécurité du périmètre? Vous aurez besoin de savoir si l'installation comporte un mur, clôture, chiens, caméras de surveillance, tourniquets, et autres systèmes de périmètre de sécurité. Ce sont que les moyens de dissuasion que vous pourriez avoir à traiter à l'extérieur. Une installation bien gardée aura couches de sécurité secondaires que vous obtenez plus près du bâtiment.

À ce stade, vous devez savoir où sont les faiblesses dans la conception

de l'installation. S'il y a un haut mur qui agrands arbres tout autour, vous pouvez monter les branches et sauter dans le composé. Bien sûr, vous devez être physiquement agile et assez forme pour faire.

Apprenez l'emplacement des feux de sécurité et où les taches sombres ou ombres tombent. Ceux-ci peuvent fournir grandes cachettes si vous prévoyez d'avoir accès la nuit. Vous devriez également considérer dumpster diving comme un moyen d'accéder à données sensibles. Vérifiez l'emplacement des bennes ordures et si elles sont facilement accessibles. Ce serait une bonne idée de savoir quand les ordures sont collectées afin que vous puissiez faux faire partie de l'équipage des ordures.

1. Badges d'identification

Organisations utilisent badges d'identification et ID utilisateur pour surveiller et contrôler le mouvement des employés. Ils sont également utilisés pour suivre les fichiers et répertoires qu'un employé crée ou modifie. Mettre main sur un badge d'identification peut vous obliger à voler un d'un employé légitime, ou faire votre propre insigne faux. Si vous ne pouvez pas obtenir un badge d'identification, alors vos autres options seraient:

- Entre tant que visiteur et votre escorte échapper.
- Utilisez la technique talonnage, supposant que le bâtiment ne dispose pas un mantrap.
- Befriend un employé dans la zone fumeurs et les suivre que vous continuez votre conversation.
- Obtenez un uniforme faux et usurper identité un entrepreneur, vendeur ou réparateur. Si vous voulez aller all-in, puis envisager acquisition un camion de service et équipement pour vous faire paraître plus légitime.

1. systèmes de détection d'intrusion

Ces facteurs comprennent généralement détecteurs de mouvement et alarmes d'intrusion.

Vous devrez connaître les types de détecteurs de mouvement vous traitez. Sont-ils infrarouge, base de chaleur, forme d'onde, capacité, photoélectrique ou détecteurs de mouvement audio passif? Chacune de ces œuvres différemment et comprendre ses forces et ses faiblesses vous aidera dans votre mission.

Vous aurez également besoin de connaître le type d'alarme intérieur du

bâtiment. L'installation peut avoir capteurs sur les portes et fenêtres, détecteurs de bris de verre, capteurs d'eau, et ainsi de suite. Alors que certaines alarmes sont destinées à informer silencieusement la sécurité d'une violation potentielle, d'autres sont conçues pour dissuader ou repousser l'attaquant. Une alarme de dissuasion ferme les portes et active les serrures pour sceller tout et tout le monde. Une alarme répulsive fait beaucoup de bruit et émet de la lumière vive pour essayer de forcer un attaquant hors du bâtiment.

Contrôles techniques

Ce sont généralement concentrés sur le contrôle d'accès car il est la zone la plus vulnérable de la sécurité physique. Les contrôles techniques comprennent les cartes à puce et les caméras de vidéosurveillance.

1. cartes à puce

Ces puces électroniques ont des circuits intégrés et qui traitent des données et permettent une authentification à deux facteurs. Les cartes à puce contiennent des informations des employés et les domaines de l'installation où ils sont autorisés / non autorisés à accéder. Avoir la carte seule ne vous aura accès à une installation. Un scanner biométrique et NIP / mot de passe doivent également être utilisés pour l'authentification. Cependant, les cartes à puce ont certaines vulnérabilités.

Une méthode de contourner les cartes à puce est par *génération de défaut*. C'est là où l'ingénierie inverse du cryptage afin de trouver la clé de cryptage et accéder aux données stockées. Cela implique parfois des erreurs de calcul en modifiant la fréquence d'horloge et la tension d'entrée ou en modifiant les variations de température.

Vous pouvez également utiliser une attaque à canal latéral pour comprendre le fonctionnement de la carte sans la détruire. Cela implique l'exposition de la carte à des conditions différentes : travers une analyse électromagnétique, analyse de puissance différentielle, et synchronisation.

Autre façon est d'utiliser un logiciel pour effectuer une attaque non invasive. Cela implique le piratage des commandes logicielles et le chargement qui vous permettent d'extraire des données de compte. Enfin, il existe un procédé connu sous le nom *micro-sondage*. Ceci est une attaque intrusive qui consiste à relier des sondes directement sur la puce. L'objectif est de prendre la puce et remettre à zéro ici.

1. Camérasvidéosurveillance

La norme de surveillance vidéo est camérasvidéosurveillance. Ils sont situés à des endroits stratégiques et sont surveillés par des agents de sécurité assis dans une salle de contrôle. Cependant, il y a toujours des taches aveugles à exploiter, vous devez donc savoir où ceux-ci sont. Les caméras peuvent être sans fil ou sur Web, ce qui signifie que vous pouvez pirater l'alimentation de la caméra et manipuler les images sont affichées sur l'écran ou brouiller le signal.

Sécurité physique est un élément essentiel de la sécurité cybernétique. Les pirates informatiques chercheront toujours à toute faiblesse qu'ils peuvent trouver, que ce soit en ligne ou hors ligne.

Chapitre 5:ingénierie sociale

Saviez-vous que l'année 2016, les trois principales préoccupations cyber-menaces étaient ingénierie sociale, menaces internes et menaces persistantes avancées? Cela vous montre à quel point les attaques d'ingénierie sociale sévissent sont devenues en cybersécurité.

Pourquoi pensez-vous ingénierie sociale est numéro un sur cette liste? Un pirate est censé attaquer le système réseau, alors pourquoi ils concentrent sur un autre aspect du système de sécurité d'une organisation?

La réponse réside dans le peuple. La plus grande faiblesse de tous les éléments de sécurité sont les personnes impliquées. Nous avons vu dans le dernier chapitre comment la technologie plus avancée ne peut vous protéger contre les cyberattaques si les personnes gardaient le bâtiment dorment au travail. Grâce à ingénierie sociale, vous pouvez pirater les gens en gagnant leur confiance et les exploiter pour les informations vous avez besoin. Cependant, vous aurez besoin d'un certain degré d'audace et d'habileté pour amener les gens à vous faire confiance, étant donné que vous êtes un étranger.

Un aspect de ingénierie sociale est qu'il est généralement fait avec un hack de sécurité physique. L'objectif est de prendre contact avec une personne qui a des informations spécifiques qui peuvent vous aider à accéder aux fichiers ou ressources de votre cible.

Par exemple:

- Envoyer la cible un email contenant des liens. Quand ils cliquent sur le lien, des logiciels malveillants ou un virus est téléchargé sur leur ordinateur, vous permettant ainsi de contrôler le système et acquiescer à vos données.
- Si vous êtes un employé dans une entreprise et vous voulez obtenir un accès non autorisé à des données confidentielles, vous pouvez informer le service de sécurité que vous avez perdu votre badge d'accès. Ils vous donneront les clés pour entrer dans la salle vous permettant ainsi d'obtenir les fichiers physiques et numériques que vous voulez.
- Vous pouvez usurper l'identité d'un fournisseur de produit authentique et prétendre que votre entreprise a besoin de mettre à jour ou installer un correctif sur le logiciel du client (par exemple logiciel de comptabilité). Vous pouvez alors demander à donner le mot de passe administrateur. Sinon, vous pouvez

simplement leur demander de télécharger le logiciel faux, qui vous donnera accès distance au réseau de la cible.

Ces exemples peuvent sembler trop simple ou facile, mais rappelez-vous que l'ingénierie sociale est la tactique la plus utilisée par les pirates pour violer la sécurité cybernétique. En apprenant comment les pirates malveillants commettent leurs exploits, vous êtes mieux placé pour empêcher votre propre système, ou d'autres, d'être piraté.

Stratégies ingénierie sociale

Examinons en détail quelques-unes des stratégies que les pirates utilisent lors d'une attaque d'ingénierie sociale.

1. Gagner confiance

Une des meilleures façons de construire confiance pour un outil d'ingénierie sociale est à travers des mots et des actions. Vous devez être articulé, fort, et être un bon causeur. Il y a aussi où un ingénieur social échoue dans sa mission parce qu'ils ont été négligents dans leur discours ou ont agi nerveusement. Cela arrive souvent quand le pirate affiche les signes suivants:

- Parler trop ou montrer trop d'enthousiasme
- répondre nerveusement en réponse à des questions
- Poser des questions bizarres
- sembler pressé
- donner des informations ayant seulement été réservées aux initiés
- Parler des gens dans la haute direction de l'organisation
- Pretendre comme ils ont du pouvoir dans la société

Tant que vous pratiquez de bonnes compétences en ingénierie sociale et techniques, vous serez en mesure de cacher ces signes.

Une tactique très efficace à utiliser pour gagner la confiance de quelqu'un est de sortir de votre façon de faire une faveur à quelqu'un et demander immédiatement un retour. Une autre tactique est quelque chose que vous avez probablement vu dans un film. Vous définissez quelqu'un en créant un problème particulier pour eux. Lorsque la victime crie à l'aide, vous précipitez sur la scène et les enregistrez. Cela fonctionne pour créer un lien entre vous et la cible potentielle.

Un travail de fausse carte d'identité et un uniforme peuvent parfois vous aider à usurper l'identité d'un employé dans une entreprise, vous permettant ainsi d'entrer dans l'établissement non détecté. Les gens vont même vous donner des mots de passe et autres informations sensibles aussi longtemps que vous semblez être un d'entre eux.

1. Phishing

Les pirates qui utilisent des attaques d'ingénierie sociale sont en mesure d'exploiter leurs cibles utilisant la technologie car il est plus facile et plus amusant. Les gens peuvent être très naïfs surtout quand ils sont en ligne. Il est tout simplement incroyablement facile de faire confiance. Les gens sont en ce

jour et âge de plus des cyberattaques.

Phishing consiste à envoyer des emails ciblés qui semblent provenir d'une source légitime ou de confiance. L'objectif est de les amener à partager des informations sensibles ou personnelles soit en envoyant directement ou en cliquant sur des liens.

L'email ressemblera à la vraie affaire de la cible visée mais c'est parce que vous avez falsifié l'adresse IP pour afficher une adresse email qui semble authentique. Vous pouvez faire semblant d'être un ami, parent ou collègue et leur demander de vous envoyer leurs renseignements personnels.

Vous pouvez également faire semblant d'être une institution financière et leur demander de cliquer sur le lien afin de mettre à jour leurs informations de compte. Quand ils cliquent, ils seront dirigés vers un faux site Web qui reflète le vrai. Comme ils se connectent, vous pouvez accéder à leurs noms d'utilisateur, ID utilisateur, mots de passe, numéro de compte bancaire, ou numéro de sécurité sociale.

Spamming est une autre tactique que vous pouvez effectuer. Vous venez leur envoyer une tonne de courriels et attendre qu'ils deviennent curieux et ouverts au moins à l'un d'eux. Le courriel contiendra une demande de téléchargement en échange de certaines informations personnelles : un cadeau gratuit (ebook, vidéo, coupon, etc.).

Une des figures les plus courantes consiste à prétendre être un fournisseur de logiciel vérifié. Tout ce que vous avez à faire est d'envoyer la cible un correctif logiciel par email et leur demander de télécharger gratuitement. Ce qu'ils ne réalisent pas est que le logiciel est fait un cheval Troie ou porte dérobée qui vous permet d'avoir un contrôle complet de leur système.

Les outils de phishing fonctionnent si bien parce qu'ils sont très difficiles à retracer au pirate. Les outils que les ingénieurs sociaux utilisent, par exemple, les réexpéditeurs et les serveurs proxy, fournissent un anonymat suffisant pour les empêcher d'être découverts.

Comment prévenir une ingénierie sociale Hack

Comme un pirateherbe, vous êtes probablement plus intéressés à apprendre comment effectuer une attaque plutôt queprévenir. Cependant, comme nousdisions au début,piratage peut travaillerfois pourbien et pourmal. Il est donc important que vous compreniez comment une attaque peut être évitée afin que vous pouvez conseillerun clientconséquence. Ces informations seront également vous aiderréaliserexploits plus efficaces. Après tout, il n'y a pas besoin de perdretemps eténergieattaquer la cibleutilisant une technique qu'ils ont déjà protégé contre.

Organisations utilisent généralement deux techniques pour empêcheringénieurs sociaux d'exploiter leurs vulnérabilités:

- 1. développement etapplicationpolitiques strictes** - L'organisation peut créerhiérarchies deinformation, oùutilisateurs sont autorisés à accédercertainesmais pas toutesdonnées. Il devrait égalementavoirapplication stricte de porterbadges d'identification par tousemployés et consultants, et chaque invité doit être escorté parsécurité. Lorsqueemployés licenciés,traitants ou fournisseurs quittent les lieux, ils doivent être dépouillés de leurs papiersidentité. Le même motpasse doit pas être utilisé pendant plus d'une durée déterminée. Enfin, dans le cas où un comportement ou manquement suspect est détecté, il doit y avoir une réponse rapide par le personnel de sécurité. L'aspectplus important de toute politiqueorganisation estrespect. Les personnes concernées doivent comprendre les exigences et les suivre en tout temps.
- 2. Formation des utilisateurs en sensibilisationla sécurité** - plupartemployés ne savent pas quoi faire quand ils sont confrontés à une attaque d'ingénierie sociale. Il doit y avoir une sorte de sensibilisation des utilisateurs etformation afin d'enseignergens comment identifier et répondre aux pirates. Cette formation doit être continue plutôt qu'un événement ponctuel. Le programme de formation devrait être assez facile pour ceux qui ne sont pas techniquement d'esprit pour comprendre. Il est également important pourgestionnaires supérieurs à donner l'exemple et s'engagent aussi la formation.

Depuisattaques d'ingénierie sociale ne sont pas seulement destinés aux organisations, nous devons examiner commentindividus peuvent se protéger. Certains des moyens de prévenir ce genre d'attaque comprennent:

1. Évitez donner des mots passe à genshasard.
2. Évitez envoyer vos informations personnelles par email ou médias sociaux sans vérifier l'identité du récepteur. Assurezvous que vous savez qui vous envoie une demande d'ami ou connexion sur Facebook, LinkedIn, ou Twitter.
3. Évitez télécharger pièces jointes partir adresses IP non identifiées, ou cliquant sur liens dans courrier spam.
4. Évitez la tendance à passer votre curseur sur un lien email. pirates informatiques sont mesure d'intégrer logiciels malveillants dans un lien et déclencher un téléchargement moment la souris passe dessus. Anti-Malware est un bon moyen d'éviter ce type de hack.

La vérité est que si ingénierie sociale peut être un peu compliqué à enlever, empêche il est également très difficile. Une organisation ne peut pas contrôler toutes les personnes liées en tout temps, et tant qu'individus, chacun a sa propre faiblesse unique. Il est votre travail pour trouver et exploiter.

Chapitre 6: Piratagemotspasse

Une des façons les plus communes pour assurer la sécurité de vos données est mot de passe-protéger. Nous sommes devenus tellement habitués à mettre motspasse dans tous nos appareils numériques que nous croyons fait que cette mesure est suffisante pour garder nos informations toute sécurité.

Cependant, la vérité est très différente. motspasse font un bon travail de garder utilisateurs non autorisés d'un système mais comme nous savons tous, pirates malveillants ont été motspasse ayant une fissuration journalière sur terrain. Dans la plupart des cas, un utilisateur peut même pas rendre compte que quelqu'un autre est courant de leur motspasse. motspasse peuvent rendre gens sentiment sécurité, mais il y a un certain nombre de vulnérabilités en leur qu'un pirate peut facilement exploiter.

Types de vulnérabilités de mot de passe

Il y a généralement deux types de vulnérabilités de mot de passe: *User* et technique.

Vulnérabilités de utilisateur

Vulnérabilités de utilisateur sont les faiblesses qui résultent de l'absence de politiques de mot de passe approprié ou la faible application de ces lignes directrices. Par exemple, combien de fois vous avez vu quelqu'un utiliser le même mot de passe pour leur ordinateur portable, smartphone, tablette, et tous leurs appareils numériques? Imaginez quelqu'un utilisant le même mot de passe pour leur Yahoo, Gmail, LinkedIn, Facebook, et Twitter! Il n'y a pas besoin d'imaginer parce que c'est exactement ce que beaucoup font!

La majorité des gens trouvent simplement trop difficile à mémoriser chaque mot de passe unique. Nous vivons dans un monde de complaisance, sorte de beaucoup juste pour regarder les plus rapides et plus faciles à faire avancer les choses. Cela traduit généralement par gens répéter le même mot de passe pour tous leurs comptes. Malheureusement, cela a simplement fait le travail des pirates beaucoup plus facile.

Avec toutes les lettres et chiffres disponibles pour utilisation, il existe potentiellement trois milliards de combinaisons de mot de passe, huit caractères. Pourtant vous seriez surpris du nombre de personnes qui choisissent des mots de passe faibles et stupides juste pour rendre plus facile le hachage. Certains même ne savent pas mot de passe et sauter le processus tout fait!

Alors quelles sont quelques-unes des vulnérabilités des utilisateurs qu'un pirate peut tirer profit?

- mots de passe qui ne sont jamais modifiés. quand remonte la dernière fois vous avez changé votre mot de passe Twitter ou courriel? Pourquoi passer par les tracas, non?
- Le même mot de passe utilisé dans plusieurs comptes différents travers différents réseaux et systèmes.
- mots de passe trop simples et sont liés à votre nom, emplacement, école, emploi, et ainsi de suite. beaucoup d'utilisateurs regardent juste la salle lorsqu'on lui demande de créer un mot de passe. Peu importe ce qu'ils voient est ce qu'ils vont utiliser. Cela peut paraître drôle mais il est vrai.
- mots de passe qui sont longues et complexes sont généralement écrits sur des morceaux de papier ou stockés dans un fichier. Tant

que l'emplacement du fichier est non sécurisé, il peut être volé.

Vulnérabilités techniques

Exploitation des vulnérabilités des utilisateurs est généralement la première étape pour un pirate informatique. Après cela, vous essayez de voir s'il y a des faiblesses techniques que vous pouvez tirer profit. Les plus courantes sont:

- non-utilisation d'applications qui masquent le mot de passe car il est tapé sur l'écran. Bien que la plupart des applications cachent immédiatement les caractères dactylographiés sur l'écran, certains ne le font pas. Si un utilisateur n'a pas configuré les paramètres de manière appropriée, ils se laissent vulnérables aux *surfeurs d'épave* (ce est expliqué plus loin).
- utilisation de programmes ou de bases de données pour stocker tous vos mots de passe, mais défaut d'obtenir la base de données appropriée. Certains utilisateurs stockent tous leurs mots de passe dans un MS Word, Access ou fichier Excel mais ne parviennent pas à sécuriser le document lui-même.
- utilisation de bases de données non chiffrées accessibles par grand nombre de personnes non autorisées. Cela est souvent le cas avec les organisations.
- utilisation de techniques de cryptage faibles par les éditeurs de logiciels et développeurs. La plupart des développeurs ont tendance à avoir trop grande confiance dans le fait que leurs codes source sont inconnus. Ce qu'ils ne réalisent pas est que avec assez de temps et patience, tout pirate expérimenté peut fissurer un code source. Un pirate qui a assez de puissance de calcul peut même utiliser des outils conçus pour pirater des chiffrements faibles.

Comprendre Motpasse cryptage

Un motpasse est dit être crypté lorsqu'il est stocké dans un système utilisant un cryptage ou un moyen algorithme de hachage. Une fois le motpasse est haché, un utilisateur voit tout est une chaîne cryptée de longueur fixe. L'hypothèse base est qu'une fois un motpasse a été haché, il ne peut pas être fissuré. LINUX va encore plus loin et ajoute une valeur aléatoire (un sel) au mot de passe haché, juste pour rendre plus sûr. Le sel est ce qui permet à deux personnes d'utiliser le même motpasse exactement encore génèrent valeurs de hachage totalement différentes.

Il y a un certain nombre d'outils qui peuvent être utilisés par pirates pour casser motpasse. Ces outils fonctionnent en prenant plusieurs motpasse bien connus, les exécuter par un algorithme de hachage, puis générer hash crypté. Une fois les hash chiffrés ont été générés, l'outil les compare au mot de passe qui doit être craqué. Bien sûr, ce processus se produit à une vitesse très rapide, et le motpasse est fissuré le moment le hachage original et la correspondance de hachage cryptée.

Parfois un pirate peut trouver un motpasse qui est très complexe et forte. Ces motpasse sont assez difficiles à craquer, mais avec les bons outils, le temps et patience suffisante, tous motpasse peuvent être piraté. Si vous voulez vous assurer que votre système estabri des pirates, vous devez obtenir les mêmes outils qu'ils utilisent, rechercher votre système pour vulnérabilités et les corriger.

Outils-Cracking Motpasse

Il y a beaucoup d'outils avancés sur le marché ce moment pour craquer des mots de passe. Certains sont plus populaires que d'autres à cause de leur efficacité à travers divers systèmes et logiciels d'exploitation. Par exemple:

- **Ophcrack** - Cet outil est utilisé pour craquer des mots de passe dans les applications Windows.
- **Caïñ et Abel** - C'est un des outils les plus efficaces. Il peut être utilisé pour craquer des hash, des mots de passe VNC et Windows, et bien d'autres applications.
- **John the Ripper** - C'est l'un des plus connus et aimés programmes pour craquer des mots de passe. Il combine un style dictionnaire d'attaque avant de lancer une attaque de force brute totale. Il est utilisé pour craquer des mots de passe LINUX et des mots de passe Windows hachés.
- **Brutus** - Cet outil fonctionne bien pour craquer des connexions pour HTTP, FTP, etc
- **Elcomsoft Distributed Password Recovery** - Cet outil fonctionne extrêmement rapidement en intégrant un programme d'accélération vidéo GPU et utilisant des milliers d'ordinateurs du réseau même temps. Il est capable de fissurer Windows, Adobe, iTunes et d'autres applications.
- **Elcomsoft System Recovery** - Cet outil utilise un CD de démarrage pour réinitialiser les droits administrateur sur un système Windows.

Il y a beaucoup d'autres outils que vous pouvez utiliser pour pirater des mots de passe sur une variété d'applications, systèmes et réseaux. La chose la plus importante est de comprendre comment fonctionne le chiffrement et comment ces outils peuvent être utilisés pour surmonter le chiffrement.

Techniques de craquagemotspasse

Nous avons tous essayé à un moment donné pour casser un motpasse. Cela aurait pu être l'ordinateur la maison, dans le laboratoire de école, ou peut-être l'appareil d'un ami. Il est probable que vous avez utilisé une méthode classique plutôt qu'une avancée. Les techniques ci-dessous sont une combinaison de certaines approches vieille école et des méthodes haute technologie.

1. **Deviner** - Ceci est probablement une des techniques plus galvaudée. Il est également l'approche simple puisque la plupart des utilisateurs ont tendance à choisir des motspasse dont ils se souviendront facilement. Tout ce que vous devez faire est logique d'utiliser pour deviner ce qui peut avoir été utilisé pour créer leur motpasse. Cette technique fonctionne mieux lorsque vous connaissez la cible ou ont un accès facile à leurs données personnelles. Le motpasse est souvent le nom de l'utilisateur ou un membre de la famille, leur carte d'identité, leur anniversaire, ou même leur animal préféré.
2. **Piquage** - C'est là où vous main autour d'une personne qu'ils clè dans leur motpasse. Vous pouvez regarder les caractères à l'écran ou mémoriser leurs frappes. Il est important que vous mélangiez pour éviter la détection, et être discret sur vos mouvements. Si vous souhaitez obtenir un motpasse des personnes dans un lieu public comme un café, vous pouvez placer une caméra dans un endroit stratégique pour surveiller leurs frappes de connexion.
3. **Ingénierie sociale** - Que faire si vous pourriez obtenir un motpasse en demandant simplement pour cela? La grande majorité des gens ont tendance à croire ce qu'on leur dit particulier si elle est dans un cadre officiel. Vous pouvez littéralement avoir accès aux dossiers des employés de partout ces jours, grâce aux médias sociaux et sites Web de l'entreprise. Un pirate peut usurper l'identité d'un membre du personnel du service informatique d'une entreprise, appeler un utilisateur, et les informer de quelques accroc techniques du système de messagerie. Le pirate demande alors que l'utilisateur leur donne leur motpasse pour régler le petit problème.
4. **Attaque de dictionnaire** - C'est là où un programme est utilisé pour créer une liste de mots de dictionnaire de texte qui

peut être comparé au motpasse réel. Il implique hachantmots en texte brut, salage, puis les comparer au mot de passe de l'utilisateur. Le mot qui correspond est alors considéré comme le mot de passe de l'utilisateur.programmes qui peuvent vous aiderlancer une attaque**dictionary** comprennent *John the Ripper*, *LophtCrack* et *Caïn etAbel*.

5. **Attaques de force** - Cela ne devrait jamais être votre premier choix en matière de craquageun motpasse. Il est une technique inefficace et extrêmement chronophage. Il est considéré comme une option de repli qui est utilisé lorsque toutesautres méthodes ont échoué. Il est principalement utilisé pour cassermotspasse6 caractères ou moins,qui estraisonlaquelle vous êtes toujours conseillé de faire vos motspasse8 caractères ou plus. Pluscaractères qu'un utilisateur met dans son motpasse, plus il est difficilese fissurerutilisant une attaque par force brute. Cependant, une attaque de force brute est très exhaustive,qui signifie que tôt ou tard le motpasse sera fissuré. Malheureusement, personne ne peut prédire quand cela se produira.programmes qui utilisent cette technique comprennent *John the Ripper*, *Rarcrack* et Oracle.

Les méthodes cidessus sont les moyenssimples etplus couramment utilisés pour cassermotspasse. Il existeautres approches qui sont disponibles, par exemple,matrice etmotpasse de probabilité tables arc en ciel. Cependant, pour un débutant, ce serait tout simplement trop complexes pourici.

Utilisant John the Ripper et pwddump3 pour casser un motpasse

L'outil **pwdump3** est un moyen efficace pour extrairemotspassepartirune basedonnées hachés Security Accounts Manager. John the Ripper, comme indiqué précédemment, peut travailler surdeux motspasse Linux et Windows. Cette procédure exige que vous avezaccès administratif.

Si vous essayez de casser un système Windows, procédezsuit:

1. Sur l'ordinateur, allez surlecteur C. Créer un répertoire et appeler«motspasse. »
2. Assurezvous que vous disposezun outil de décompression (tel que WinZip) installé sur l'ordinateur.cas contraire, puis téléchargez et installez.

3. Télécharger pwdump3 et John the Ripper et les installer immédiatement. Les extraire dans le répertoire créé cidessus.

4. Tapez la commande

c: passwordspwdump3> cracked.txt

La sortie de cette étape seramotpassecomptessécurité Windows Gestionnaire hash, qui sera ensuite capturé dans le fichier txt.

1. Tapez la commande

c: craked.txt passwordsjohn

Ceci lancera John the Ripper contre les hashes, et la sortie seront les mots de passe utilisateur fissurés. Cependant, ce processus peut prendre un temps très long, selon la complexité des mots de passe et le nombre d'utilisateurs du système.

Si vous Cracking un système LINUX, utilisez la procédure suivante:

1. Télécharger les fichiers source pour LINUX.

2. Tapez la commande

[root @ yourcurrentfilename hôte local] #tar - xzf john - 1.7.9.tar.gz

Cela va extraire le programme et créer un répertoire / src.

1. Dans le répertoire / src, tapez la commande

make générique

1. dans le répertoire / Exécuter, tapez la

commande./ unshadow / etc / passwd / etc / shadow> cracked.txt

Le programme unshadow sera utilisé pour fusionner fichiers masqués et mots de passe et les dans le fichier txt.

1. Tapez la

commande:./ John cracked.txt

Cela va lancer le processus craquage, qui peut également prendre un certain temps. La sortie devrait être la même que pour la procédure Windows.

Création mots passe sécurisés

En ce qui concerne renforcement la sécurité des données dans une organisation, il devient nécessaire d'embaucher un chapeau blanc pour aider concevoir de meilleures politiques de mot de passe. L'objectif est d'enseigner aux utilisateurs du système comment créer des mots de passe plus sûrs, ainsi que les effets d'une mauvaise sécurité des mots de passe. Pour les personnes qui veulent obtenir leurs renseignements personnels, les mêmes techniques peuvent également s'appliquer dans la plupart des cas.

Les critères à suivre comprennent:

- mot de passe formé qui combine lettres majuscules et minuscules, chiffres, symboles et caractères spéciaux.
- Ajout de signes de ponctuation entre mots séparés
- Délibérément mots fautes d'orthographe
- Changer des mots tous les 12 mois. En cas de violation de sécurité, les mots de passe doivent être changés.
- Veiller à ce que les mots de passe soient de longueurs différentes pour rendre plus difficile l'effraction.
- stocker des mots de passe tous dans un programme de gestion de mot de passe plutôt qu'un non garanti MS Excel, Access ou fichier Word.
- Éviter la tendance à recycler des anciens mots de passe.
- Veiller à ce que les mots de passe ne soient pas partagés du tout, pas même avec amis ou des collègues au travail.
- Verrouillage du BIOS système aide un mot de passe
- Etablir des méthodes d'authentification plus avancées, par exemple, certificats numériques ou cartes à puce.

Pour pirater un mot de passe, vous devez comprendre ce qu'est un mot de passe fort ou faible ressemble. Avoir la bonne connaissance de la façon de créer un mot de passe vous aidera à devenir un hacker plus efficace.

Chapitre 7: Réseau sans fil Attacks

Réseaux sans fil sont devenus tellement banals nos jours, mais malheureusement, ils sont aussi très vulnérables aux menaces piratage. Cela est dû au fait qu'ils impliquent la transmission de données par fréquences radio, rendant ainsi informations susceptibles être interceptées. Dans cas où l'algorithme de chiffrement est faible ou données transmises sont non chiffrées, la situation devient bien pire.

Attaques WLAN

Il y a plusieurs façons qu'une attaque réseau sans fil peut être lancée. Ceux-ci comprennent:

1. Association Unintentional

Il y a cas où un réseau sans fil chevauche un autre, permet un utilisateur de sauter inadvertance d'un dans l'autre. Si un pirate malveillant profite de cela, ils pourraient acquérir information contenue dans un réseau qu'ils ne visent à être sur en premier lieu.

1. Réseaux non conventionnels

Ces réseaux qui ne sont pas la sécurité appropriée qui est habituellement réservé pour ordinateurs portables et points d'accès. Ils ont tendance à être faciles pour pirates. Ils comprennent imprimantes sans fil, lecteurs de codes barres, périphériques Bluetooth et PDA.

1. Des attaques déni de service

Ce type d'attaque consiste à envoyer certaines ou milliers de messages, commandes ou demande à un point d'accès. En fin, le réseau est forcé de tomber panne ou utilisateurs sont empêchés d'accéder au réseau.

1. Man-in-the-middle

Cette attaque implique un hacker utilisant leur ordinateur portable pour agir comme un point d'accès doux et attirer utilisateurs. Le pirate connecte leur point d'accès doux au point d'accès réel travers une carte sans fil différent. Utilisateurs qui tentent d'atteindre le véritable point d'accès sont donc obligés de passer par le point d'accès doux. Cela permet au pirate de saisir toutes informations sont transmises dans le réseau. Attaques Man-in-the-middle sont habituellement effectuées dans parties communes qui ont des hotspots sans fil.

1. Usurpation d'identité MAC

Cela peut être décrit comme vol de l'identité d'un ordinateur qui possède des privilèges du réseau. Un pirate tente de voler l'adresse MAC

(Media Access Control) d'un ordinateur autorisé par logiciel coursexécution que « renifle » it out. Une fois le pirate trouve ces ordinateurs administratifs et leurs papiers d'identité, ils utilisent d'autres logiciels qui leur permettent d'utiliser ces adresses MAC.

Vérification des réseaux sans fil

La majorité des réseaux sans fil sont sécurisés par mot de passe afin de contrôler la façon dont les utilisateurs accèdent et utilisent le réseau. Deux façons d'authentifier un réseau sans fil *Wired Equivalent Privacy (WEP)* et *Wi-Fi Protected Access (WPA)*.

Wired Equivalent Privacy (WEP)

WEP offre la plus grande intimité d'un réseau câblé et crypte toutes les données transmises sur un réseau. Cependant, en raison de ses nombreuses vulnérabilités, il a été largement remplacé par WPA.

Cracker un réseau WEP peut se faire soit active ou passive. Fissuration active est plus efficace, provoque une surcharge du réseau, et est donc plus facile à détecter. Fissuration passive, d'autre part, ne modifie pas le trafic jusqu'à ce que le réseau a été fissuré.

Les outils que vous pouvez utiliser pour casser un réseau WEP incluent:

- **wepcrack** - Ceci est un outil open-source que vous pouvez télécharger à partir de wepcrack.sourceforge.net.
- **Aircrack** - Cet outil vous permet de renifler un réseau, et peut être téléchargé à partir de aircrack-ng.org
- **WebDecrypt** - Cet outil utilise un dictionnaire pour générer des clés WEP. Il peut être téléchargé à partir de webdecrypt.sourceforge.net
- **Kismet** - Ceci est un outil qui peut être utilisé à plusieurs fins différentes, comme renifler les paquets réseau, détecter les réseaux visibles et invisibles, et aussi identifier les intrus.

Wi-Fi Protected Access (WPA)

Cette authentification a été conçue pour surmonter les faiblesses du WEP. Cela dépend de la phrase de chiffrement des paquets utilisant des touches temporelles. Une faiblesse du WPA est qu'il est vulnérable aux attaques de dictionnaire si des phrases faibles sont utilisées. Les outils de craquage WPA comprennent:

- **Cain et Abel** - Cet outil décode les fichiers reniflés par d'autres programmes
- **CowPatty** - Cet outil utilise des tactiques de force brute pour casser des clés pré-partagées

Comment MAC spoofing Attacks

Un des moyens les plus populaires de prévenir une MAC attaque par usurpation consiste à utiliser filtrage MAC. Un filtre MAC est utilisé pour bloquer adresses MAC non autorisées de joindre un réseau sans fil, même si l'utilisateur a le motpasse. Cependant, il est un moyen efficace de bloquer un pirate déterminé.

Dans l'exemple ci-dessous, vous apprendrez à usurper l'adresse MAC d'un utilisateur qui a l'autorisation de se connecter à un réseau. Assurez-vous que votre adaptateur Wi-Fi est en mode de surveillance. Les outils qui seront utilisés sont *Airodump-ng* et *macchanger*.

1. Avec adaptateur en mode de surveillance, tapez la commande

Airodump-ng -c [channel] [routeur cible MAC Adresse] -bssid -I wlan0 mon

Cela vous permettra de détecter la cible réseau sans fil. Tous utilisateurs qui utilisent le réseau seront affichés dans une fenêtre popup, y compris leurs adresses MAC autorisées.

1. Choisissez une des adresses MAC à utiliser comme votre propre adresse. Cependant, vous devez d'abord éteindre l'interface de surveillance. Tapez la commande

Airmon-ng arrêter wlan0 mon

1. Vous devez alors éteindre l'interface sans fil de l'adresse MAC que vous avez choisi. Tapez la commande

ifconfig wlan0 vers bas

1. Maintenant il est temps d'exécuter le logiciel *Macchanger*. Tapez la commande

macchanger -m [Nouvelle adresse MAC] wlan0

1. Allumez l'interface sans fil de l'adresse MAC que vous aviez choisi. Tapez la commande

ifconfig wlan0 up

Vous avez changé avec succès votre adresse MAC à celle d'un utilisateur autorisé. Connectez-vous au réseau sans fil et voyez si vous êtes mesuré de se connecter.

Comment sécuriser un réseau sans fil

Il y a un certain nombre d'approches que vous pouvez utiliser pour sécuriser un réseau sans fil. Chaque hacker éthique doit connaître ces conseils afin qu'ils puissent empêcher pirates malveillants d'exploiter vulnérabilités du système. Ceux-ci comprennent:

- Installer parefeu, anti-virus et anti-spyware. Assurez-vous que tous vos logiciels de sécurité est mis à jour et le parefeu est activé.
- Chiffrez vos stations de base, routeurs et points d'accès en brouillant vos communications réseau. Ces appareils sont fabriqués avec commutateurs de chiffrement, mais ils sont mais sont généralement éteints. Assurez-vous que vous activez la fonction de chiffrement.
- Modifier le mot de passe par défaut du routeur sans fil. Veillez à ce qu'ils soient longs et complexes.
- Éteignez le réseau chaque fois qu'il est pas utilisé.
- Éteignez le diffuseur d'identification du routeur, qui est la façon dont l'appareil diffuse sa présence. Cela est inutile puisque les utilisateurs réels savent déjà qu'il existe.

Chapitre 8: Piratage un Smartphone

Ce chapitre couvrira la procédure que vous pouvez suivre pour pirater un smartphone Android. Vous devrez télécharger des logiciels spécialisés de tiers légitimes parties afin de rendre le processus plus facile et plus rapide.

Cette procédure est totalement anonyme et vous serez en mesure d'accéder à toutes les données dans le téléphone de la cible. Il est une exploitation à distance qui est effectuée via une connexion Internet sécurisée.

Étapes à suivre:

1. Allez sur le site MasterLocate (*MasterLocate.com*) pour utiliser l'application en ligne. Vous ne devez pas télécharger le logiciel sur votre ordinateur ou téléphone pour utiliser. L'outil vous permettra de suivre la position GPS en temps réel de la cible, surveiller leurs SMS et messages WhatsApp, écouter leurs appels et garder trace de leur compte Facebook.
2. Exécutez l'application MasterLocate sur votre téléphone ou ordinateur.
3. Une boîte de dialogue devrait apparaître avec le classement terrain. *numéro mobile de votre cible* Entrez le numéro de la cible ici. Assurez-vous que le téléphone de la cible est en ligne lorsque vous faites cette étape.
4. Dans la même boîte de dialogue, juste en dessous de la *Numéro mobile de votre cible*, du champ il y a *Vérifier*. l'onglet Lorsque vous cliquez dessus, le programme tentera d'établir une connexion. Attendez que le pays de la cible à venir.
5. Une fois la connexion est établie et vérifiée, allez sur le côté droit de la boîte de dialogue. Parcourez la *Rapports* section pour afficher messages, journaux d'appels et fichiers de la cible. Si vous voulez télécharger quoi que ce soit sur votre appareil, cliquez sur *Exporter Méthode*. Cela vous présentera des options pour les formats de téléchargement, comme .zip et .rar.

Cette méthode de piratage smartphones est simple et directe. Tout ce que vous devez faire est d'assurer que vous et la cible sont en ligne tout au long du

processus de piratage informatique. Toute interruption de la connexion Internet arrêtera le processus. autre chose est que vous devez connaître le numéro de téléphone de la victime ainsi que leur numérotéléphone mobile code pays.

Smartphone Hacking contremesures

Tant que votre téléphone est connecté à un réseau Wi-Fi non sécurisé ou contient des logiciels malveillants compromis, il est vulnérable à l'exploitation par des pirates. Alors, quelles sont quelques-unes des mesures qui peuvent être prises pour obtenir un Smartphone contre des pirates malveillants?

1. Assurez-vous que votre téléphone est sous l'exécution d'un antivirus fiable, à jour et mis à jour.
2. Connectez-vous uniquement pour sécuriser la connexion Wi-Fi lorsque vous naviguez sur Internet, en particulier dans des lieux publics. Ces endroits sont de meilleurs terrains de chasse d'un pirate informatique pour avoir volé des données des victimes sans méfiance. Wi-Fi publique ne doit pas être utilisé pour des activités qui nécessitent d'entrer vos coordonnées de compte bancaire, par exemple, des achats ou des services bancaires.
3. Évitez la tendance à télécharger des applications qui demandent l'accès à vos renseignements personnels.
4. Assurez-vous que votre système d'exploitation est constamment mis à jour, automatiquement ou manuellement.
5. Si vous avez des doutes quant à la source d'un logiciel, laissez-le seul. Seulement acheter ou télécharger des magasins d'applications vérifiées. Découvrez ce que les commentaires disent de mieux pour comprendre ce que d'autres utilisateurs ont utilisé.
6. Verrouillez votre téléphone chaque fois que ce n'est pas utilisé. Assurez-vous que votre mot de passe est fort et change régulièrement.
7. Si vous recevez des messages texte contenant des liens, ne cliquez pas sur le lien, surtout si vous ne connaissez pas l'expéditeur. Il est préférable de supprimer ces messages de spam dès qu'ils entrent dans votre téléphone. Les pirates informatiques ont tendance à envoyer des textes à des milliers d'utilisateurs de téléphones prétendant être des entreprises légitimes ou des sites Web. Lorsque le lien est cliqué, un logiciel malveillant est installé sur le téléphone, permet ainsi des données à accéder.

Il y a des milliards de téléphones mobiles dans le monde entier, ce qui en fait une zone de piratage informatique qui offre le plus rapide et le plus facile d'attaquer une cible. La plupart des gens ont tendance à se méfier quand ils sont sur leurs ordinateurs, mais ils ont tendance à baisser leur garde

lorsnavigation sur leur téléphone. Il est donc extrêmement important
quegens restent vigilants en tout temps.

Chapitre 9: Piratage Conseils pourdu débutant

Vousacheté ce livre parce que vous vouliez apprendre certaines des compétences fondamentales et techniques pourpiratage. Ne seraitil une honte si vous avez fini par se Busted, ou pire encore, piraté par un pirate informatique compagnon avec plusexpérience?

Il est très important que vous assurezvous que vous prenez soin extrême lorsdémarrage. Oui, il y a beaucoup de plaisir lorsque vous commencez à voir les résultats de votre travail, mais vous devez comprendre comment manœuvrer et nedéTECTÉS.

Voici cinq conseils clés que tousdébutants devraient suivre:

1. éviter le piège deachatlogicielspiratage de sites Webhasard. Il y a milliers d'arnaqueurs qui prétendent avoirlogiciels etoutils qui sont « garantis » au travail, mais ceuxci sont généralement misplace pour attirerpirates débutants. Vous perdrez votre argent en échange de logiciels inutiles. Vous pouvez même avoir vos propres données personnelles volées ainsi. Assurezvous que vous neaffaire avecsites Web légitimes ou vérifiés. Faites vos recherches bien et savoir ce queautres pirates utilisent et où ils les reçoivent de.
2. Évitez la tentation de télécharger freeware de l'Internet. Ceuxci comprennentpluparttemps keyloggers et chevauxTroie. Si vous êtes sérieuxsujetpiratage, vous devez être prêt à dépenserpeuargent pour obtenirchoses qui fonctionne. Le meilleur etplus efficacelogiciels est pas libre. Être un radin et aller pour les freebies vous exposer à pirates d'escroquerie malveillants qui ne manqueront pas d'exploiter votre système.
3. Lorsachatoutilspiratage, essayez d'utiliser Bitcoins. Il y a quelques outils que vous ne voulez pas faire remonter à vous, par exemple,serveurs privés virtuels, anonymes VPS et serveurs d'enregistrement de domaine. Si vous utilisez votre carte de crédit personnelle, vous pouvez vous exposer à plus d'un, et une vérification rapide de votre compte révélera vos activités de piratage. Le meilleur coup est de toujours garder votre véritable identité distincte de vos activitésligne.
4. Apprenez à développer vos compétences. Si vous êtes

qualifiés dans développement web seul, alors vous devrez apprendre programmation. Si vous êtes un programmeur, puis apprendre écriture de script. L'objectif est de savoir quelque chose sur tout plutôt que d'obtenir l'aise d'être dans une boîte.

5. Il est OK au début d'utiliser le logiciel d'autres personnes pour lancer vos attaques. Cependant, chaque pirate apprend à sa valeur son s'il tôt ou tard comment écrire ses propres codes, programmes et scripts. Si vous pouvez créer vos propres outils de piratage, alors vous aurez passé à l'étape suivante et de là vers être un hacker élite.

Conclusion

Nous sommes arrivés à la fin d'un long voyage à travers le monde du hacking. Si vous ne saviez pas qu'il y a soit sur le sujet, alors vous devriez avoir suffisamment de connaissances maintenant pour commencer à réaliser de petits exploits.

Il y a beaucoup de potentiel dans le piratage, et ce ne sont pas tous des malveillants. Apprendre à pirater est effectivement la meilleure façon de rester sécurisé dans un monde où la vérification de votre email est dangereuse, et parler à cet étranger mignon peut conduire à plus que ce que vous attendiez (et non pas une bonne façon)!

Que ce soit un appareil mobile ou un ordinateur de bureau, la vigilance totale doit être maintenue. Les pirates sont toujours à l'affût, alors vous devez apprendre leurs trucs et contre-attaquer. Tant que ce guide de piratage éthique, ce livre vous a montré les premières étapes pour le piratage, ainsi que vous protéger.

Continuez à apprendre et appliquer ce que vous avez appris ici. Rappelez-vous de rester sécurisé en tout temps, et ne pas en faire votre tête.

Bonne chance!

Resources

www.csoonline.com

www.giac.org

www.whitehatsec.com

www.sans.org

www.2-spyware.com